IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
WICHITA FALLS DIVISION

UNITED STATES OF AMERICA

v.

RICKY DALE HOWARD (01)

NO. 7:21-CR-008-O

CERTIFICATION OF DATA COPIED FROM AN ELECTRONIC DEVICE, STORAGE MEDIUM, OR FILE PURSUANT TO FED. R. EVID. 902(14)

I, Syretha Mcleod-Long, attest under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I was employed by the Federal Bureau of Investigation (FBI) in the position of Forensic Examiner from June 2012 until July 2019 with the North Texas Regional Computer Forensic Laboratory ("NTRCFL"). I held an FBI certification to conduct digital forensics. Since 2019, I have worked as a Senior Cyber Security Forensic Specialist for Blue Cross Blue Shield. By reason of my former position and specialized training, I am authorized and qualified to make this declaration as a "qualified person" under Fed. R. Evid. 902(14).

I further state:

1. The items I am certifying are e01 image files created by FTK Imager v.3.3.0.5 & v.4.2.0.13. FTK Imager is software used to acquire data that is stored on electronic data storage devices such as hard drives, in a forensically sound manner. This means that an exact copy of the data stored on the hard drive is created without any alterations to the original data. FTK Imager was used to create e01 (Encase Image File Format) images of submitted items DL106752_1 and DL108565_1. FTK Imager also verifies that the image of the data is created

successfully by producing an alphanumerical hash value. FTK Imager was installed on forensic imaging / exam stations F5405940 and F2673180, assigned to me and located at the North Texas Regional Computer Forensics Lab (NTRCFL).

F

2. I have been requested to verify the authenticity of the data that I copied from an internal hard drive in a Gateway Model SX2802 desktop computer, to wit: a Western Digital hard drive, serial number WCASY7950929, performed on February 5, 2018 and saved to Storage Area Network (SAN) Storage. I can verify that on February 5, 2018, I received the Gateway Model SX2802 desktop computer, with an internal Western Digital hard drive, serial number WCASY7950929, inside a sealed evidence container bag labeled R2-18-7072. The internal Western Digital hard drive, serial number WCASY7950929 was identified with NTRCFL internal number DL106752_1. On this same date, I used FTK Imager v. 3.3.0.5 to create an e01 image of the hard drive, which was created successfully. Below are the image verification results that I am certifying based upon verified matching hash values:

   NTRCFL Evidence Item, labeled DL106752_1:

   a. Hash:
      i. MD5: 998a819909b4a746192b35590bb58857
      ii. SHA1: f381c3fbd438022e8159ad1356b12c24dcfdf450
   b. Model: Western Digital hard drive
   c. Serial Number: WCASY7950929

3. I have been requested to verify the authenticity of the data that I copied from an internal hard drive in an Acer Model 5251-1513 laptop computer, with serial number LXPWJ020010171DE3B1601to wit: a Seagate hard drive, serial number 6VC3W0G0, performed on September 25, 2018 and saved to SAN storage. I can verify that on September 25, 2018, I received the Acer Model 5251-1513 laptop computer, with serial number LXPWJ020010171DE3B1601, containing an internal Seagate hard drive, serial number 6VC3W0G0, inside a sealed evidence container bag labeled R2-18-7304. The internal Seagate hard drive, serial number 6VC3W0G0 was identified with NTRCFL internal number DL108565_1. On this same date, I used FTK Imager v. 4.2.0.13 to create an e01 image of the Seagate hard drive, serial number 6VC3W0G0, which was created successfully. Below are the image verification results that I am certifying based upon verified matching hash values:

NTRCFL Evidence Item, labeled DL108565_1:

d. Hash:
   i. MD5: f26349afc7574598d7b57833b9a72dde
   ii. SHA1: dfda1edb9dff2bad2ce918fffa2cb70210728146
e. Model: Seagate hard drive
f. Serial Number: 6VC3W0G0

4. The hash values taken during imaging essentially runs each bit of data stored on the device through an algorithm (common algorithms include MD5 and SHA1) as it is copied onto the destination drive. This hash then serves as a digital "fingerprint" for the data, and may be verified at any time by running the data through the algorithm again. Verification that the data has not been altered in anyways is demonstrated when the resulting value is identical to the has taken during acquisition.

5. For purposes of Fed. R. Evid. 902(14), I certify that the data that I acquired from : (1) internal hard drive in a Gateway Model SX2802 desktop computer, to wit: a Western Digital hard drive, serial number WCASY7950929; and (2) internal hard drive in an Acer Model 5251-1513 laptop computer, serial number LXPWJ020010171DE3B1601to wit: a Seagate hard drive, serial number 6VC3W0G0 was copied identically and that this data is authenticated by the above-referenced hash values, which are a process of digital identification. I further certify that the evidence being offered in this case is the same as that retained by the NTRCFL and can be verified as such by the above-referenced hash value.

I further state that this certification is intended to satisfy Fed. R. Evid. 902(14).

SIGNATURE 7/13/21 DATE